

JUNIPER NETWORKS AND ORACLE DELIVER SIMPLE AND SECURE REMOTE ACCESS FOR MISSION-CRITICAL APPLICATION ENVIRONMENTS

Challenge

Provide authenticated, secure, and policy appropriate access to network applications and resources for all remote users anytime, anywhere, from any device.

Solution

Juniper Networks SA Series SSL VPN Appliances and Oracle Identity Management solutions work together to deliver a seamless, clientless, single sign-on and secure access environment for any type of remote user and any type of device. Network application and corporate resource access policies are enforced.

Benefits

- Reduces overall costs of business operations
- Improves user productivity
- Mitigates risk and helps meet regulatory and compliance obligations
- Integrated solution provides lower TCO for managing identity lifecycle and enforcing user access to networks resources and applications

Providing remote access to enterprise applications requires security without compromise – application protection regardless of location and type of device. Today’s diverse universe of users, from mobile employees to contractors and partners, requires anywhere, anytime access to the very enterprise applications that require the most stringent security policies. Providing this access becomes even more challenging when you consider that across, and even within, each of these user communities, network access policy is often stored on multiple security systems.

The Juniper Networks SA Series SSL VPN Appliances and Oracle Identity Management Solution

Juniper Networks® SA Series SSL VPN Appliances integrate seamlessly with both Oracle’s Identity and Access Management Suites to provide seamless and secure access to all Oracle mission critical applications. The combined solution helps customers manage the end-to-end lifecycle of user identities both local and remote, mitigate online risk and fraud, and enable seamless secure access and enforcement with granular authorization policies. Together Oracle and Juniper Networks not only increase overall network and application security, but provide lower total cost of ownership, speed application deployment, and deliver granular protection to enterprise resources for mobile and remote users anywhere, anytime, and from any device.

Juniper Networks Secure Access for Mobile and Remote Employees

SA Series appliances enable organizations of all sizes to deploy cost-effective secure remote access for mobile and remote employees. The use of SSL, the security protocol found in all standard Web browsers, eliminates the need for client-software deployment and costly ongoing client maintenance and support when compared to traditional IPsec solutions for remote access. The appliances’ browser-based approach enables mobile users to access corporate network resources securely from any machine, including unmanaged endpoints such as Internet kiosks and mobile devices like PDAs. The SA Series appliance authenticates each user’s identity, verifies the health of the endpoint device before network access is granted, and dynamically authorizes access to only necessary resources, as determined by user identity, as well as machine and network integrity.

The SA Series Host Checker verifies both prior to establishing and during a session that a device has an acceptable security posture, such as requiring enabled and up to date endpoint security applications (antivirus, personal firewall, current system patch levels, etc.). This health check process ensures that the endpoint device meets corporate security policy requirements before and after granting network access. If corporate policy isn’t met then the device and user can self remediate or be quarantined when necessary.

The hardware-accelerated SA Series appliances provide superior performance, reliability, and ease-of-management to fulfill all enterprise remote employee and partner access requirements. This is why it has consistently maintained leading market share and is deployed in the largest and most demanding enterprises across every vertical worldwide.

Oracle Identity Management

Oracle's best-in-class suite of Identity Management (IdM) solutions allows enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall. The Oracle Identity Management Suite is leading the next wave of Identity Management with an application centric approach, enabling Oracle solutions to interoperate with all major enterprise systems such as directories, email, databases, and ERP systems to ensure enterprise-wide security for all applications.

The Oracle Access Management Suite is the only integrated solution offering next-generation technologies that enable risk-based authentication, proactive online fraud prevention, and fine-grained authorization, as well as best-of-breed functionality including web access management and identity federation.

Policy-driven Access Management for Juniper Networks Secure Access Users

Oracle Access Manager (OAM) can be used to provide a policy-driven way to control user access to HTTP resources, including Web pages, directories, Web applications and J2EE resources such as Java server pages, EJBs, and servlets. Juniper Networks SA Series appliances

provide SSO to OAM protected resources via a standards-based SAML interface to the Oracle Identity Federation (OIF) product. Other resources can also be protected including standalone Java/C++/C programs, ERP, and CRM applications. This integration allows the SA Series to check a user's access policy in order to determine if a requested application is protected and to determine the appropriate authentication mechanism needed to be enforced.

Multi-factor Authentication and Fraud Prevention with Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) provides strong mutual authentication security in a pure Web environment. In addition, the OAAM provides real-time risk scoring for initiation and in-session transactions to identify fraud at multiple "gateways" or checkpoints—pre-, post-, and in-session authentication. The absence of hardware and software dependencies satisfies the ease of implementation, low-cost, and efficiency requirements of large-scale enterprises, while providing the broad-based security coverage users demand.

Together, the Juniper Networks SA Series SSL VPN Appliances and Oracle's Adaptive Access Manager provide enterprises with a best-in-class, integrated and seamless remote access control solution with strong multi-factor authentication and advanced real time fraud prevention capabilities to enable the most flexible and secure access to the enterprise's most mission-critical applications.

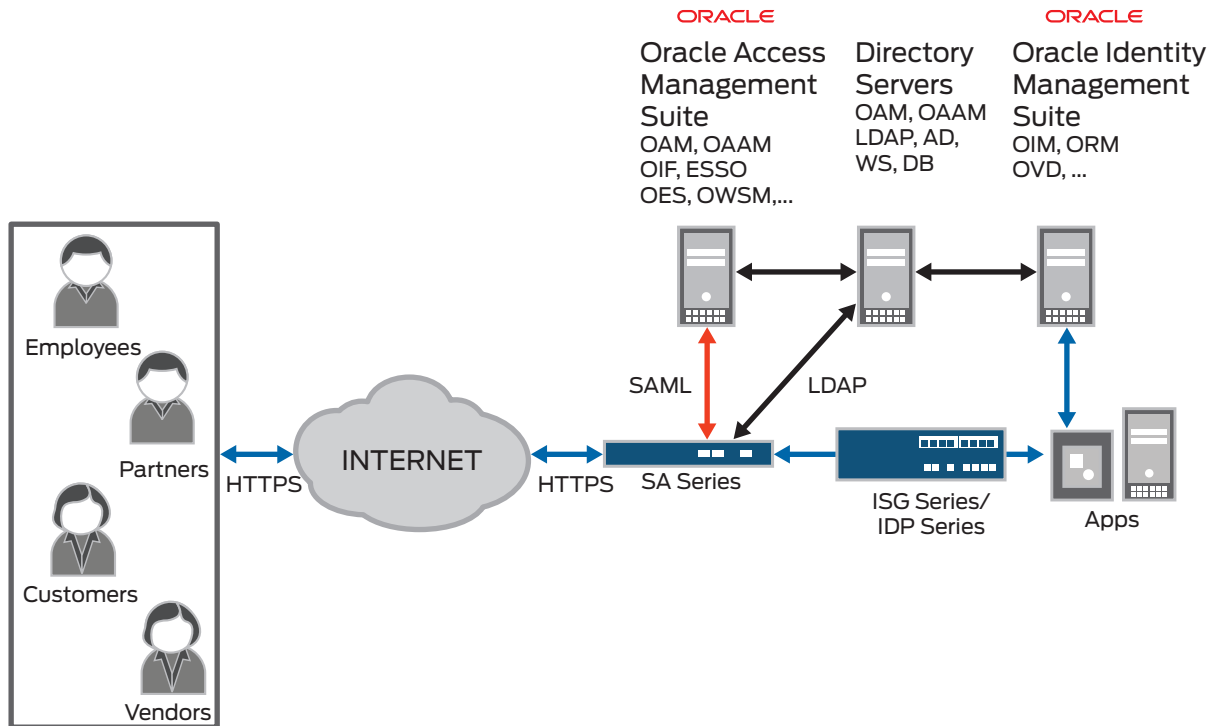


Figure 1: Secure Remote and Extranet Partner Access with Oracle Identity Management Suite

Authentication and Authorization of SA Series Appliance Users When User Identity Profile is “Split” Among Different Repositories

Real-time aggregation of user data that is “split” in multiple data repositories is accomplished with Oracle Virtual Directory (OVD), Juniper enables authentication and authorization of remote users with SSL VPN. OVD provides an LDAP interface for the SA Series appliance to communicate with multiple user repositories. This lowers the cost of operations by facilitating the SSL VPN solution to have seamless access to identity data stored in non-LDAP repositories.

Provisioning and De-Provisioning SSL VPN Users

When a new user is created through the Oracle Identity Manager, the user can immediately access authorized applications, through the Juniper Networks SA Series appliance. The SA Series enables password management against LDAP, allowing user self-service, for events like password reset, to reduce helpdesk and support requirements. When that user’s access must be terminated, SSL VPN access is immediately revoked when their profile is marked as such via Oracle Identity Manager. This allows enterprises to manage large numbers of user accounts across heterogeneous systems and applications, including SSL VPN access for remote users whether they be employees, partners, suppliers, or contractors. The combined solution lowers cost of operations by automating the user account provisioning/de-provisioning process, while dramatically lowering the risk associated with enforcing access rights for newly provisioned or de-provisioned users.

Enterprise SSO for Desktop Applications for SSL VPN users

Remote users can achieve Single Sign-On (SSO) to both Web-based and client/server applications via the SA Series SSL VPN Appliance. SSO allows users to gain quick and easy access when logging on to networks, applications, and Web sites as users have just one password to remember. This increases productivity and improves ease of use. SSO also lowers user support costs by virtually eliminating password-related support calls.

Leading SSL VPN Solutions that Protect Your Investment and Enterprise Applications

Juniper Networks is the SSL VPN market share leader and an innovator of secure Access Control Solutions. Because Juniper Networks SSL VPN solutions interoperate with all leading user identity/access management systems and support multi-vendor switches/access points, your investments as well as your enterprise applications are protected.

This integrated offering of highly acclaimed products from two of the industry’s leaders and visionaries offers the highest return on your investments with improved security, lower administrative costs, high scalability, and the backing of industry leaders.

To learn more about policy enforcement techniques to protect your network or to learn more about the SA Series product family, please visit www.juniper.net/sa-series or contact your Juniper Sales Representative.

About Oracle

Oracle is the world’s largest enterprise software company. For more information about Oracle, visit our Web site at www.oracle.com.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King’s Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airsides Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.